IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA v. ARTEM MIKHAYLOVICH LIFSHITS, Defendant.	Case No. 1:20-mj-256

AFFIDAVIT IN SUPPORT OF
A CRIMINAL COMPLAINT AND ARREST WARRANT

I, Heather Turner, being duly sworn under oath, do hereby depose and state:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the United States Secret Service ("USSS") and have been so employed since July 2015. I have a number of different duties, including being responsible for investigating violations of the federal code, including wire fraud and aggravated identity theft. As a Special Agent, I have received specialized training and instruction in the field of financial crimes and fraud investigations.

2. This affidavit is submitted in support of a criminal complaint and arrest warrant charging the defendant, ARTEM MIKHAYLOVICH LIFSHITS (Лифшиц Артём Михайлович) ("LIFSHITS"), with conspiracy to commit wire fraud, in violation of Title 18, United States Code, Section 1349.

3. The facts and information contained in this Affidavit are based on my training and experience, on information provided to me by other members of USSS and other law enforcement officers, court records and documents, business records, interviews, publicly available information, and my review of physical and documentary evidence. I have personally

participated in the investigation of the offense set forth below and, because of my participation and review of evidence gathered in the case, I am familiar with the facts and circumstances of this investigation. Because this Affidavit is limited in purpose, I am not including all facts known to law enforcement concerning this investigation.

4. Below, I will explain the relevant statutes and the technical aspects of the investigation. I will then briefly describe Project Lakhta's past and continuing efforts to influence the United States political system. I will summarize an indictment obtained in the District of Columbia and a criminal complaint obtained in the Eastern District of Virginia, which charged several Project Lakhta members for their role in conspiring to defraud the United States and in using the means of identification of United States persons to open bank accounts, PayPal accounts, and cryptocurrency accounts.

5. I will also explain the USSS's more recent investigation into Project Lakhta members' use of the means of identification of United States persons to open cryptocurrency accounts. The remainder of the Affidavit will focus on LIFSHITS, who has been a manager in Project Lakhta's Translator Department since at least January 2017. The evidence below establishes that LIFSHITS was a manager in a unit responsible for much of Project Lakhta's influence operations and that these operations are ongoing. The evidence also establishes that LIFSHITS operated cryptocurrency accounts opened in the name of United States identity theft victims for personal gain.

RELEVANT STATUTES AND BACKGROUND

6. *Wire Fraud and Conspiracy to Commit Wire Fraud.* Title 18, United States Code, Section 1343 provides, in relevant part, that whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or

fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be guilty of a federal offense. Title 18, United States Code, Section 1349 provides, in relevant part, that whoever attempts or conspires to commit wire fraud shall be guilty of a federal offense.

7. *Aggravated Identity Theft*. Title 18, United States Code, Section 1028A provides, in relevant part, that whomever, knowingly and unlawfully transferred, possessed, or used a means of identification of another person during and in relation to an enumerated felony in Sections 1028A(c) or 2332b(g)(5)(B), shall be guilty of a federal felony. Wire fraud and conspiracy to commit wire fraud, are both enumerated felonies in Section 1028A(c).

TECHNICAL BACKGROUND

8. *Bitcoin*. Bitcoin is a cryptocurrency, which is a specific type of decentralized digital currency for which transactions are effected via cryptography. Bitcoin is often used in e-commerce or in the purchase of goods or services from online merchants. Each Bitcoin address is controlled through the use of a unique, corresponding private key — that is, a cryptographic password needed to access the address. Only the holder of the private key (or keys) for an address can authorize any transfers of Bitcoin from that address to other Bitcoin addresses. Bitcoin addresses are often stored alongside their corresponding private keys in digital "wallets." No identifying information about the payor or payee is transmitted in a Bitcoin transaction, as generally only the Bitcoin addresses of the parties are needed for the transaction. However, all Bitcoin transactions are recorded on a digital blockchain, which is a publicly available ledger that, among other things, records the source wallet address, the receiving wallet address, and the amount transacted for every Bitcoin transaction. Accordingly, as a general

matter, the Bitcoin blockchain contains a certain and verifiable public record of every single Bitcoin transaction ever made.[1] Moreover, because the blockchain is distributed among thousands of computers, it is effectively impossible to edit or delete the blockchain's record of completed transactions.

9. *Bitcoin exchanges*. A user typically acquires Bitcoin from a Bitcoin exchange. Bitcoin exchanges generally accept payments of conventional currency, and, for a fee, transfer a corresponding number of Bitcoin to the customer or convert Bitcoin back into fiat currency. Bitcoin exchanges can also provide Bitcoin wallet services, although an individual can obtain a wallet from a number of sources, such as downloading software from the internet. United States law requires Bitcoin exchanges operating within the United States to register with the Financial Crimes Enforcement Network ("FinCEN"), an arm of the Department of the Treasury, and as such, are required to follow certain money transmitter regulations.[2]

10. *Regulation of Bitcoin exchanges*. Based on my research and experience, the types of Bitcoin exchanges can vary from large, established, and licensed businesses that operate under and follow strict know-your-customer ("KYC") and Anti-Money Laundering ("AML") policies to unlicensed individuals operating without regard to the United States federal regulations governing virtual currency exchanges. Individuals involved in criminal activity often prefer to use unregulated and unlicensed exchanges to purchase Bitcoin with unlawful proceeds or cash out Bitcoin acquired through illegal activity, precisely because these exchanges do not request and store the type of information required under KYC and AML guidelines. Though operating

[1] There are third-party services that can obfuscate the wallets involved in transactions; however, these methods are not relevant to this case because the transactions discussed in this Affidavit were identified on the public blockchain.

[2] *See* https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering (accessed August 27, 2020).

independently of the larger, more established exchange companies, the independent exchanges will often have active accounts with these larger companies due to the convenience and amount of resources (i.e., Bitcoin and fiat currency) available to their customers.

11. *Blockchain analysis*. Though Bitcoin affords a significant degree of anonymity to its users, there are a number of investigative tools exists that law enforcement can use to track the flow and location of Bitcoin, including blockchain analysis (also referred to as "Bitcoin tracing"). Blockchain analysis or Bitcoin tracing is a process whereby those wishing to do so can use the blockchain to follow Bitcoin transactions from Bitcoin addresses to Bitcoin address. This enables the public to, among other things, identify a point of entry—that is, the Bitcoin address in which Bitcoin purchased from fiat currency is first stored—and the point of exit—that is, the Bitcoin address out of which Bitcoin is exchanged for cash.

PROBABLE CAUSE

A. Background on Project Lakhta and Efforts to Interfere with United States Political System

12. Since at least 2014, known and unknown individuals, operating as part of a broader Russian effort known as "Project Lakhta," have engaged in political and electoral interference operations targeting populations within the Russian Federation and in various other countries, including, but not limited to, the United States, members of the European Union, Ukraine, and Africa. Since at least May 2014, Project Lakhta's stated goal in the United States was to disrupt the democratic process and to spread distrust towards candidates for political office and the political system in general.

13. Beginning in or around mid-2014 and continuing to the present, Project Lakhta obscured its conduct by operating through a number of Russian entities, including, but not limited to, the Internet Research Agency LLC, Internet Research LLC, MediaSintez LLC,

GlavSet LLC, MixInfo LLC, Azimut LLC, NovInfo LLC, Nevskiy News LLC (a/k/a "NevNov"), Economy Today LLC, National News LLC, Federal News Agency LLC (a/k/a "FAN"), and International News Agency LLC (a/k/a "MAN"). These entities employed hundreds of individuals in support of Project Lakhta's operations with an annual global budget of millions of United States dollars.

14. In furtherance of its goals, Project Lakhta members traveled to the United States to collect intelligence; established United States computer infrastructure; and built the capacity to reach millions of United States citizens through social media accounts operated under fictitious personas, including through the use of political advertisements. Further, Project Lakhta members acquired fake identification documents (such as driver's licenses) to further their operations and used stolen United States identities to open accounts with banks and cryptocurrency exchanges.

B. Overview of the Wire Fraud Conspiracy and LIFSHITS' Role in the Conspiracy

15. During the course of the investigation into Russian interference in the United States political system, law enforcement obtained evidence establishing that Project Lakhta members purchased the means of identification of United States persons. Project Lakhta members then used these means of identification to open bank accounts, PayPal accounts, and cryptocurrency accounts. The United States persons did not provide permission for their means of identification to be sold or used for such purposes. Further, and as explained below, the fraudulently opened accounts deprived the banks, PayPal, and the cryptocurrency exchanges of the right to control their property and exposed the entities to potential economic losses.

16. LIFSHITS applied for a job with Project Lakhta in and around July 2015. By in and around January 2017, LIFSHITS served as the head of Project Lakhta's Translator Department.[3]

17. From in and around April 2014, Project Lakhta's Translator Department focused on influencing the United States population. The Translator Department conducted operations on social media platforms, such as YouTube, Facebook, Instagram, and Twitter. The Translator Department's primary goal was to sow discord in the United States political system, incite civil unrest, and polarize Americans by promoting socially divisive issues, with particular emphasis on racial divisions and inequality in the United States

18. The evidence outlined below establishes that LIFSHITS accessed a cryptocurrency account that was opened using the means of identification of a real United States person. This cryptocurrency account was setup with a United States-based cryptocurrency exchange ("Exchange 1"). This United States person did not provide LIFSHITS or any other person permission to use his means of identification for this purpose. Then, on at least one occasion, LIFSHITS sent a payment of Bitcoin from this account to his personal account with Exchange 3, which is another United States-based cryptocurrency exchange. In accessing and using the fraudulently opened cryptocurrency account, LIFSHITS and his co-conspirators deprived Exchange 1 of its right to control its property and exposed Exchange 1 to potential economic losses.

[3] This is a translation from Russian, and it could be referred to as a Department, Unit, or Project. The USAO-DC Indictment, which is discussed in Section C, refers to it as the Translator Project.

C. The District of Columbia Indictment and Elena Khusyaynova Criminal Complaint in the Eastern District of Virginia

19. On February 16, 2018, a grand jury in the District of Columbia returned an Indictment charging thirteen Russian nationals and three Russian companies, including the Internet Research Agency, with committing federal crimes, while seeking to interfere with United States elections and political processes, including the 2016 presidential election. Indictment, *United States v. Internet Research Agency, et al.*, 1:18-CR-32 (DLF) (D.D.C. Feb. 16, 2018) (hereinafter the "USAO-DC Indictment"). *See* Attachment A. As of the filing of this Complaint, only Concord Management and Consulting LLC, which was one of three Russian companies indicted, had appeared in United States courts to defend itself.[4]

20. The USAO-DC Indictment charged certain of the Project Lakhta[5] defendants with committing aggravated identity theft and conspiring to commit wire fraud. The United States charged these co-conspirators, in part, because they used the stolen identities of real United States persons to open bank accounts, PayPal accounts, and cryptocurrency accounts. Co-conspirators used some of these accounts to further the conspiracy to interfere in the United States political system and other accounts for self-enrichment.

[4] On March 16, 2020, the United States dismissed Concord Management and Consulting LLC from the Indictment. Concord "availed itself of the Court's jurisdiction to obtain discovery from the United States . . . while positioning itself to evade any real obligations or responsibility," even refusing to produce a corporate representative despite "appearing" through counsel. Mot. to Dismiss Concord Defs., 2, 6, *United States v. Internet Research Agency, et. al,* 1:18-cr-32 (DLF) (D.D.C. Mar. 16, 2020). In light of the defendant's conduct, the United States dismissed these parties from the Indictment, stating substantial federal interests were no longer served by continuing the proceedings against them. *See id.* at 9. The Indictment remains pending and active as to thirteen named individual defendants and the IRA. *Id.*

[5] While the co-conspirators worked for Project Lakhta and were thus its employees, it is also true that some, if not all, employees were paid through other business entities.

21. On September 28, 2018, Elena Alekseyevna Khusyaynova ("Khusyaynova") was charged by criminal complaint in the Eastern District of Virginia (the "Khusyaynova Complaint") for participating in a conspiracy to defraud the United States, in violation of Title 18, United States Code, Section 371. *See* Attachment B. Between April 2014 and at least September 2018, Khusyaynova, as the Chief Accountant in Project Lakhta's finance department, managed the financing of substantially all aspects of Project Lakhta's operations, which included media and influence activities directed at the United States, the European Union, and Ukraine, as well as the Russian Federation. In that role, she oversaw the budgets of various Project Lakhta entities. The affidavit in support of the Khusyaynova Complaint documents her overt acts in furtherance of Project Lakhta's goals of interfering in the United States political system, including, but not limited to, her completion and submission of detailed budgets that included funding for political advertisements on Facebook, Instagram, and other social media outlets.

22. I submit that the factual allegations in the USAO-DC Indictment and the affidavit in support of the Khusyaynova Complaint provide further probable cause to believe that LIFSHITS has conspired to commit wire fraud and committed aggravated identity theft. Both the USAO-DC Indictment and affidavit in support of the Khusyaynova Complaint are attached hereto and incorporated by reference.

D. Project Lakhta's Political Interference Activities from late December 2016 to Present in the United States

23. Between in or around December 2016 and in or around May 2018, as part of the effort to sow discord in the United States political system, Project Lakhta members used social media and other internet platforms to inflame passions on a wide variety of topics, including immigration, gun control and the Second Amendment; the Confederate flag; race relations; Lesbian, Gay, Bisexual, and Transgender ("LGBT") issues; the Women's March; and the

National Football League national anthem debate. Project Lakhta members took advantage of specific events in the United States to anchor their themes, including the shootings of church employees in Charleston, South Carolina, and concert attendees in Las Vegas, Nevada; the Charlottesville "Unite the Right" rally and associated violence; police shootings of African-American men; and the current United States administration's personnel and policy decisions.

24. Below I detail only a small portion of the overt acts committed in furtherance of the conspiracy to defraud the United States. More overt acts are thoroughly discussed in the Khusyaynova Complaint, which is incorporated by reference and is attached to this Affidavit.

25. According to evidence gathered by law enforcement, Project Lakhta leadership directed its members to create "political intensity through supporting radical groups, users dissatisfied with [the] social and economic situation and oppositional social movements." Project Lakhta members also sought, in the words of one employee, to "effectively aggravate the conflict between minorities and the rest of the population."

26. Project Lakhta members did not exclusively adopt one ideological viewpoint; rather, they wrote on topics from varied and sometimes opposing perspectives. Project Lakhta members also developed strategies and guidance to target audiences with conservative and liberal viewpoints, as well as particular social groups. For example, one Project Lakhta member directed his fellow co-conspirator in or around October 2017 that "if you write posts in a liberal group, . . . you must not use Breitbart titles. On the contrary, if you write posts in a conservative group, do not use Washington Post or BuzzFeed's titles." Using the example of individuals of color who are also employees of the LGBT community, one Project Lakhta member offered the following guidance on how to target the group:

> Colored LGBT are less sophisticated than white; therefore, complicated phrases and messages do not work. Be careful dealing with racial content. Just like ordinary Blacks,

> Latinos, and Native Americans, colored LGBT people are very sensitive towards #whiteprivilege and they react to posts and pictures that favor white people. . . . Unlike with conservatives, infographics works well among LGBT and their liberal allies, and it does work very well. However, the content must be simple to understand consisting of short text in large font and a colorful picture.

(Preliminary translation of Russian text)

27. Project Lakhta members also developed detailed analysis of timely news articles and guidance for how to describe the articles in social media posts in order to interfere with the United States political process. For example, in or around early August 2017, one co-conspirator, working under the guise of the Facebook group "Secured Borders," analyzed a large quantity of United States news articles, summarized the substance of the articles, and outlined ways for the conspiracy to promote them. Specifically, one or more co-conspirators described each article and categorized its theme, provided a strategic response with a particular focus on how to target United States audiences, and then noted approval to use the strategic response. The strategic response was referred to as "Tasking Specifics," which appeared to include an assignment to certain Project Lakhta members to disseminate the message on social media platforms.

28. For instance, citing an online news article titled "Paul Ryan Opposes Trump's Immigration Cuts, Wants Struggling American Workers to Stay Poor," from on or about August 5, 2017, a Project Lakhta member directed his fellow co-conspirator to message the article in the following way:

> Brand Paul Ryan a complete and absolute nobody incapable of any decisiveness. Emphasize that while serving as Speaker, this two-faced loudmouth has not accomplished anything good for America or for American citizens. State that the only way to get rid of Ryan from Congress, provided he wins in the 2018 primaries, is to vote in favor of Randy Brice, an American veteran and an iron worker and a Democrat.

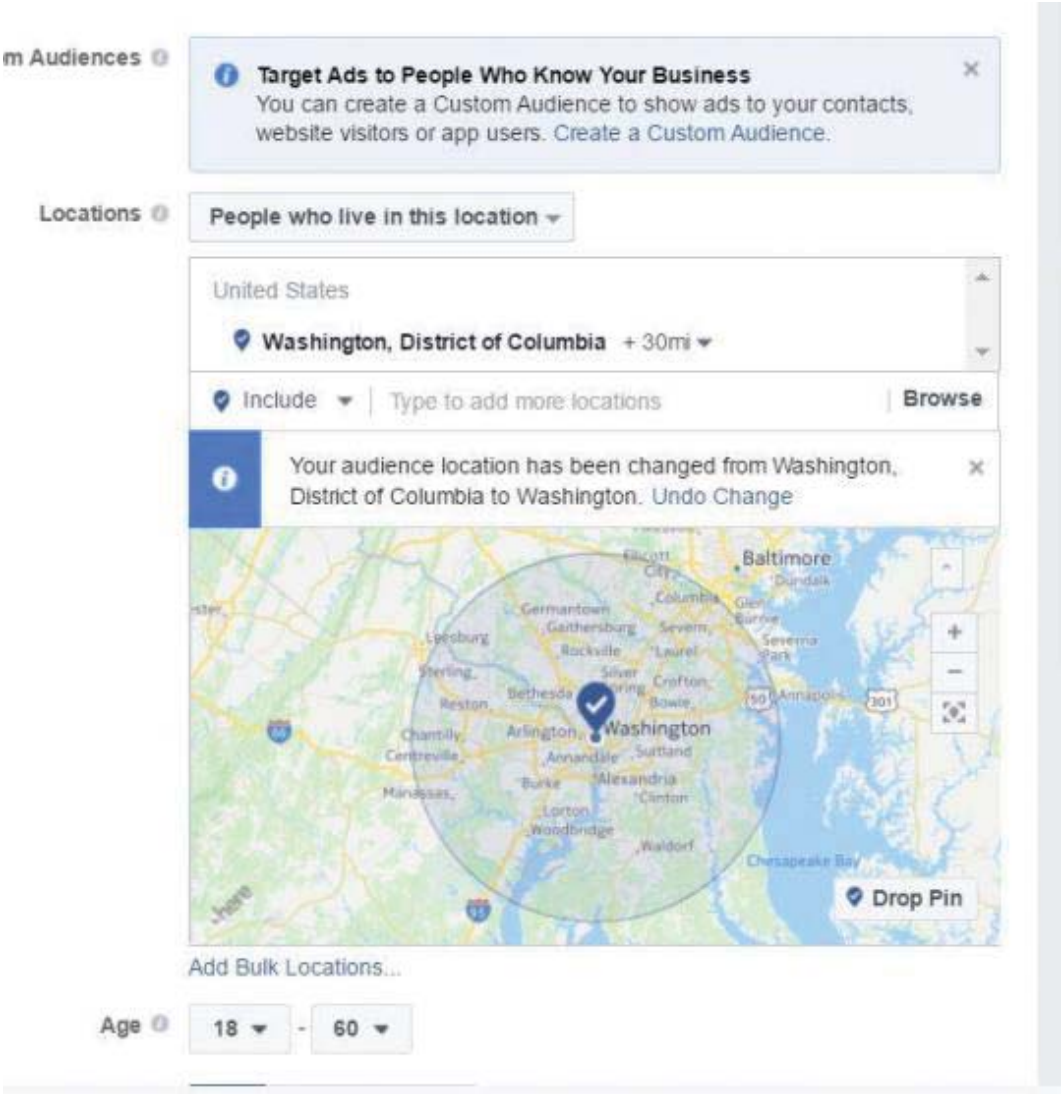
(Preliminary translation of Russian text)

29. In another example, citing an online news article titled "CNN's Pro-Jeb! Republican: Trump White House Like a 'Brothel,'" from on or about August 7, 2017, a Project Lakhta member directed his fellow co-conspirator to message the article in the following way:

> CNN commentator "RINO" likened the Trump administration to a "brothel." Mass News Media Criticism! Accuse CNN of yet another lie. State that during past elections, namely, this mainstream media, which supported Hillary Clinton's candidacy for United States President almost 100%, disseminated fake news, insulting statements, and lies about Donald Trump and his supporters. This continues now. This is precisely why such news sources as the New York Times, Washington Post, CNN, CBS, Time, and Huffington Post must not be taken seriously, for they are the main propaganda channels that are screwing with the heads of American citizens. Remind readers that each of the above-mentioned media resources supported Hillary Clinton and received funds from her election fund. They produced fake social study research results at polls predicting a Clinton win with a 10-15% lead over Trump and tried hard to insult and discredit Trump. Summarize with a statement that CNN long ago lost its reputation as a trusted source and that its reputation is still declining.

(Preliminary translation of Russian text)

30. Further, on or about July 2, 2017, a Project Lakhta member used the "Helen Christopherson" Facebook account, which is a fake United States persona, to send a United States organization a proposal to purchase advertising targeted at individuals within 30 miles of Washington, DC, including significant portions of the Eastern District of Virginia, as depicted below:



The proposed advertisements had an estimated reach of 29,000 to 58,000 individuals.

Subsequently, the United States organization agreed to make the "Helen Christopherson" Facebook account a co-organizer of the event on Facebook.

31. On or about March 22, 2018, a Project Lakhta member used the Twitter account "@johncopper16" to post the following tweet about the 2018 midterm election:

> Just a friendly reminder to get involved in the 2018 Midterms. They are motivated They hate you They hate your morals They hate your 1A and 2A rights They hate the Police They hate the Military They hate YOUR President

32. In or around July 2019, a Project Lakhta member founded Eliminating Barriers for the Liberation of Africa ("EBLA") in Accra, Ghana. EBLA employed approximately sixteen Ghanians and received direction from the Project Lakhta member. EBLA members established social media accounts on Facebook and Twitter. The EBLA members designed the accounts to look like the users were located in the United States. EBLA members used these accounts to post about racial issues in the United States. For example, one Twitter account, @africamustwake posted the following message:

> YOU POLICE BEEN KILLING BLACKS SINCE YA RAGGEDY MOMMAS GAVE BIRTH TO U. HAPPY MLK DAY TO U HYPOCRITES.

33. On or about January 25, 2020, an EBLA employee created an EBLA company page on LinkedIn and subsequently advertised a job posting seeking a chapter coordinator in Charleston, South Carolina. The advertisement described EBLA as "a network of strong advocates of human rights…we as young activists and human rights advocates envisage a better world were POC live freely, thus our call to join hands with our brothers and sisters world-wide, especially in the United States where POC are mostly subjected to all forms of Brutality." This advertisement was also posted to at least six other internet websites in late January and early February 2020. Law enforcement have identified approximately 90 social media accounts with known or suspected links to EBLA.

34. According to a CNN interview with a former EBLA employee, employees were given United States news articles to read and topics to post. The EBLA employee stated: "So you get stories about LGBT, you get stories about police brutality, depends on what you are working." The employee said that she and other employees were told that the best time to tweet and post was late afternoon and at night in Ghana, which are times when a United States audience would have been active.

35. Project Lakhta members continue to use social media platforms in furtherance of its efforts to sow discord in the United States. Further, members are using sophisticated methods to obfuscate the origins of their social media activity, including the use of virtual private servers, software enabling anonymous communications, and single use or "burner" email accounts linked to social media accounts. Law enforcement have identified social media accounts used by Project Lakhta members since August 2019 up until the present to post about a wide range of topics, including, but not limited to, the Second Amendment, Black Lives Matters, and LGBTQ issues. As previously stated, Project Lakhta members have posted about these issues for several years. The accounts associated with these posts used virtual servers located in Ghana, Cameroon, Central African Republic, Germany, Ukraine, Estonia, United States, and elsewhere.

E. Background on USSS Investigation into Project Lakhta's Use of Cryptocurrency Accounts

36. In and around October 2018, USSS began investigating Russian efforts to interfere in United States elections and democratic processes. Specifically, USSS examined how Project Lakhta members used and continue to use cryptocurrency accounts to further the objects of the conspiracy to interfere with the United States political system; and how Project Lakhta members used and continue to use accounts created using the stolen identities of real United States persons for personal enrichment.

37. In an effort to uncover the identities and activities of Project Lakhta members, USSS identified multiple cryptocurrency accounts registered to email accounts known to be used by co-conspirators. The USAO-DC Indictment identified many of these email accounts. *See* Attachment A. As set forth in the USAO-DC Indictment, Project Lakhta members used these email accounts to open fraudulent accounts with banks, cryptocurrency exchanges, and PayPal. Based on a review of the information provided in response to subpoena requests, USSS

identified several cryptocurrency accounts to be of "high interest" due to registered identifiers, transactional activity, and/or Internet Protocol ("IP") address logs on file.

38. One of the initial accounts that USSS identified was hosted at Exchange 1. The Exchange 1 account was registered to a known Project Lakhta email account, x[T.W.]x@gmail.com[6] (hereinafter the "T.W. Exchange 1 Account"). The T.W. Exchange 1 Account reflected debits to several beneficiaries, including accounts registered to LIFSHITS and another known Project Lakhta member ("Co-Conspirator 1"). The IP activity associated with the T.W. Exchange 1 Account also matched the IP address activity of cryptocurrency accounts registered to LIFSHITS and Vladimir Venkov, who is charged in the USAO-DC Indictment.

39. Law enforcement conducted a voluntary interview of T.W. T.W. confirmed that he had never purchased, owned, or possessed any cryptocurrency or virtual currency, such as those outlined in this Complaint. T.W. stated that he never authorized another person to use or sell his personally identifiable information to any other individual or organization. T.W. stated that he did not establish or use the email x[T.W.]x@gmail.com or email handle "x[T.W.]x." Thus, LIFSHITS and his co-conspirators did not have lawful authority to use T.W.'s means of identification.

40. USSS identified a second account, which was hosted at another United States cryptocurrency exchange ("Exchange 2"). The Exchange 2 account was registered to a known Project Lakhta email account, allforusa@yahoo.com (hereinafter the "AllforUSA Exchange 2 Account").[7] Project Lakhta members opened the AllforUSA Exchange 2 Account using the

[6] Here, I use T.W. instead of the actual email account in order to protect the identity of the victim. T.W. is one of the identity theft victims listed in Count 2 of the USAO-DC indictment.

[7] The USAO-DC Indictment alleges that the allforusa@yahoo.com email account was used by co-conspirators to, among other things, open fraudulent bank accounts as part of the underlying conspiracy to interfere with U.S. elections.

identifiers of T.B. According to Exchange 2's records, Project Lakhta members solely funded the AllforUSA Exchange 2 Account with an incoming credit from an account also in the name of T.B. at a United States-based financial institution. This credit was used exclusively to fund outgoing payments to a Blockchain wallet[8] that USSS investigators determined was controlled by Co-Conspirator 1. Additionally, the IP activity of the AllforUSA Exchange 2 Account again matched the IP activity of accounts registered to LIFSHITS and Venkov.

41. Law enforcement conducted a voluntary interview of T.B. T.B. confirmed that he had never purchased, owned, or possessed any cryptocurrency or virtual currency, such as those outlined in this Complaint. T.B. stated that he never authorized another person to use or sell his personally identifiable information to any other individual or organization. T.B. confirmed that he did not provide another person permission to open the accounts at issue in this Complaint. Thus, LIFSHITS and his co-conspirators did not have lawful authority to use T.B.'s means of identification.[9]

F. Identification of Accounts Used to Purchase United States Persons' Personally Identifying Information

42. Law enforcement obtained a search warrant for the contents of the email account allforusa@yahoo.com, which as stated above is associated with a cryptocurrency account linked to both LIFSHITS and Co-Conspirator 1. During a review of the emails, law enforcement located "Order Confirmation" emails received from an online criminal marketplace that sells fraudulent passports and similar identification documents (the "Criminal Marketplace"). These

[8] Blockchain is a wallet service provider ostensibly based in Luxembourg. Blockchain provides encrypted non-custodial wallet services and claims that legal process served upon Blockchain will not yield any relevant information regarding the specific user or associated transaction activity of a given wallet.

[9] T.B. is another of the identity theft victims listed in Count 2 of the USAO-DC indictment.

emails corresponded to purchases of United States driver licenses that reflected the real names, addresses, and dates of birth of United States identity theft victims. This type of personally identifiable information is a "means of identification" as defined in Title 18, United States Code, Section 1028(d)(7).

43. Project Lakhta members thus used the allforusa@yahoo.com account to, among other things, create an account with the Criminal Marketplace. Project Lakhta members then used this account to purchase fraudulent documents reflecting the identifiers of real United States persons, including T.B. The relevant order confirmations related to United States identity theft victims noted in this Complaint are listed below. I have redacted the real identifiers and the personally identifiable information of the United States persons.

Order Date	**May 4, 2017**
Order Number	12261
Total Price	$45
Payment Method	Bitcoin
Billing Address	"T.B."
Customer Details	allforusa@yahoo.com
Product	Driver's License
Identifiers	"T.B."[Real Address Redacted] [Real Date of Birth Redacted]

Order Date	**May 11, 2017**
Order Number	12373
Total Price	$30
Payment Method	Bitcoin
Billing Address	"T.B."
Customer Details	allforusa@yahoo.com
Product	Driver's License
Identifiers	"J.W." [Real Address Redacted] [Real Date of Birth Redacted]

Order Date	**July 4, 2017**
Order Number	13228
Total Price	$210
Payment Method	Bitcoin
Billing Address	"T.B."
Customer Details	allforusa@yahoo.com
Product	Driver's License

Identifiers	"T.C." [Real Address Redacted] [Real Date of Birth Redacted]

G. LIFSHITS' Connections to and Role in Project Lakhta

44. During the course of this investigation, law enforcement obtained a search warrant for an email account belonging to a known Project Lakhta member. During a review of the contents of this email account, law enforcement identified Project Lakhta rosters from January and September 2017, which identify members by department and position. The rosters also reflect the fact that Project Lakhta hid its activities by paying its members through different companies including, but not limited to, Azimut LLC. As detailed in the USAO-DC Indictment, Azimut LLC is one of several entities that Project Lakhta used to obscure its conduct.

45. LIFSHITS is listed in the Project Lakhta rosters. One spreadsheet titled "Roster of employees of Project Lakhta as of January 18, 2017," listed an "Artem Mikhaylovich Lifshits" as a "Task Manager" in "Translator Department No. 2" with a monthly salary of 70,000 rubles. A second spreadsheet titled "Roster of employees of Project Lakhta as of October 26, 2017," listed "Artem Mikhaylovich Lifshits" as a "Task Manager" in "Translator Department No. 1" with a monthly salary of 80,000 rubles. In addition, another roster dated September 2017, listed "Artem Mikhaylovich Lifshits" as "Task Manager No. 2."

46. As described more fully above, LIFSHITS, as a manager in the Project Lakhta's Translator Department, would have been directly involved in social media messages and other messages directed at and intended to influence the United States population.

47. During the course of the investigation into Project Lakhta, law enforcement obtained information indicating that LIFSHITS applied to Project Lakhta in and around July 2015. More specifically, law enforcement obtained a search warrant for an email account belonging to another known Project Lakhta member. Based on the review of emails obtained

pursuant to the search warrant, law enforcement located an email from July 2015 from LIFSHITS' known email account with a resume attached. The resume belonged to "Artem Mikhaylovich Lifshits," born December [redacted], 1992, and reported a phone number ending in 4982. These identifiers for LIFSHITS all match the information on file with Exchange 3.

H. LIFSHITS Use of Cryptocurrency Accounts and IP Addresses Known To Be Used by Project Lakhta Members

1. USSS Identification of LIFSHITS

48. While conducting a forensic transactional analysis on the T.W. Exchange 1 Account as discussed above, USSS identified LIFSHITS as a transactional counterparty. Specifically, the transactional activity of the T.W. Exchange 1 Account reflected an outgoing payment to a Bitcoin address [redacted]. Valid legal process confirmed this as an address hosted at an exchange operating in the United States ("Exchange 3") and assigned to LIFSHITS, whose full identifiers were on file with Exchange 3. These identifiers included LIFSHITS' Russian passport, email account, and telephone number.

49. During the course of this investigation, law enforcement obtained other information to corroborate that the information used to establish LIFSHITS' account with Exchange 3 is actually associated with LIFSHITS.

50. For instance, a September 2012 publication of Monok'e, which is a student magazine associated with the Faculty of Economics at Saint Petersburg State University, included a photograph of LIFSHITS and noted him to be "head" of the publication's "information committee." LIFSHITS' contact information included the phone number ending in 4982, which he used to setup his Exchange 3 account. In addition, I note that LIFSHITS' resume, which he sent to the known Project Lakhta member in 2015, listed Saint Petersburg State University in the education section.

51. In a post on Russian social networking platform VK from March 2010, user "artemous" listed a photograph, date of birth, and Russia as his country. The date of birth supplied by "artemous" matches LIFSHITS' date of birth supplied to Exchange 3. Further, LIFSHITS' passport photo supplied to Exchange 3 and the photograph of "artemous" appear to be the same person.

52. Finally, during the course of this investigation, law enforcement obtained search warrants for email accounts belonging to two known Project Lakhta members. The address books of both of these individuals included LIFSHITS' phone number ending in 4982, and referenced it as associated with "Artemka Boss" and "Troll Face."

53. Based on the above, I submit that there is at least probable cause to believe that LIFSHITS established and uses the Exchange 3 account that is registered in his name.

54. A forensic transactional review of LIFSHITS' Exchange 3 account resulted in the identification of an account registered to LIFSHITS at another exchange operating in the United States ("Exchange 4"). The account was opened using the same email account that LIFSHITS used to open his Exchange 3 account. Exchange 4 had no additional identifiers for the account. However, this email account, as well as the IP address activity associated with the account, match the registered email account and IP address activity of LIFSHITS' Exchange 3 account. As a result, I submit that there is at least probable cause to support that LIFSHITS also operates the Exchange 4 account registered in his name.

2. LIFSHITS' Use of Project Lakhta-Controlled IP Addresses

55. During the course of the investigation into Project Lakhta, law enforcement determined Project Lakhta members used Russian IP address XX.XX.XXX.218 ("Russian IP Address 1") to access a significant number of social media accounts used to develop fictitious

personas and to engage with Americans on social and political issues. LIFSHITS' account at Exchange 3 reflected over 30 instances of activity from this IP address. Further, LIFSHITS' account at Exchange 4 reflects four instances of activity from this IP address.

56. In addition, Project Lakhta members used United States IP address XX.XXX.XXX.67 ("United States IP Address 1") to access cryptocurrency accounts setup in the name of United States identity theft victims, as well as an account Project Lakhta members used to procure United States victim identifiers from the Criminal Marketplace. LIFSHITS' account at Exchange 3 reflected six instances of activity from this IP address. LIFSHITS' account at Exchange 4 reflected four instances of activity from this IP.

57. Further, the T.W. Exchange 1 Account, which as discussed above is registered to a United States identity theft victim, reflected multiple instances of activity from United States IP address XXX.XXX.XXX.22 ("United States IP Address 2"). LIFSHITS' account at Exchange 3 reflected six instances of activity from this same IP address.

58. Below is a visual representation of this activity.

United States IP Address 1

ACCOUNT LOGINS LINKED BY IP ADDRESS				
Date Range	**IP Instances**	**Account**	**(Project Lakhta) Registration Email**	**US Person Identity**
6/28/2016	11	Exchange 2	allforusa@yahoo.com	T.B.
8/9/2016	10	Exchange 2	wemakeweather@gmail.com	T.B.
8/9/2016	13	Exchange 2	mightytyrone7@gmail.com	T.C.
8/9/2016 – 9/13/2016	6	[Foreign Exchange 2]	mightytyrone7@gmail.com	T.C.
6/7/2017 – 1/14/2018	23	Exchange 1	X[T.W.]x@gmail.com	T.W.
6/9/2017 – 10/1/2017	43	[Foreign Exchange 1]	ihatecrime1@gmail.com	J.W.
8/12/2016 – 9/16/2017	99	[Foreign Exchange 1]	wokeaztec@outlook.com	A.S.
3/20/2017 – 12/29/2017	6	Exchange 3	mycryptodeals@yandex.ru	N/A – LIFSHITS
1/11/2018	4	Exchange 4	mycryptodeals@yandex.ru	N/A – LIFSHITS

United States IP Address 2

ACCOUNT LOGINS LINKED BY IP ADDRESS				
Date Range	**IP Instances**	**Account**	**(Project Lakhta) Registration Email**	**US Person Identity**
12/26/2017-12/29/2017	4	Exchange 3	mycryptodeals@yandex.ru	N/A – LIFSHITS
01/29/2017	2	Exchange 1	X[T.W.]x@gmail.com	T.W.

Russian IP Address 1

ACCOUNT LOGINS LINKED BY IP ADDRESS				
Date Range	**IP Instances**	**Account**	**(Project Lakhta) Registration Email**	**US Person Identity**
12/21/2017 – 6/6/2018	33	Exchange 3	mycryptodeals@yandex.ru	N/A – LIFSHITS
1/12/2018	5	Exchange 2	X[T.W.]x@gmail.com	T.W.
2/9/2018 – 6/6/2018	3	Exchange 4	mycryptodeals@yandex.ru	N/A – LIFSHITS

59. I submit that LIFSHITS' appearance in the Project Lakhta employee rosters, the fact that he sent his resume to a known Project Lakhta member, and his use of Project Lakhta-controlled IP addresses to access his own accounts, establishes probable cause to believe that LIFSHITS works for Project Lakhta and uses Project Lakhta-controlled IP addresses to access his Exchange 3 account.

I. LIFSHITS' Use of the T.W. Exchange 1 Account for Personal Gain

60. On or about December 29, 2017, LIFSHITS accessed and used the T.W. Exchange 1 Account to conduct an electronic transfer of funds from the T.W. Exchange 1 Account to his personal Exchange 3 account. This transaction is publicly viewable on the Bitcoin blockchain and USSS confirmed its existence through other investigative means.

61. On or about December 29, 2017, LIFSHITS used United States IP Address 1 at 15:35 UTC to access his Exchange 3 account. Then, three minutes later, he used the same IP address to access the T.W. Exchange 1 Account. This is on the same day that the T.W. Exchange 1 Account sent an electronic funds transfer to LIFSHITS' Exchange 3 account.

62. With this transaction, LIFSHITS (1) intentionally and voluntarily devised or participated in a scheme to defraud — as evidenced by controlling and using a fraudulent

cryptocurrency account, and (2) used interstate wire communications to further the fraud — as evidenced by the online cryptocurrency transactions.

1. Noteworthy Overlaps in IP Activity between the LIFSHITS and T.W. Accounts

63. Between December 26, 2017 and January 12, 2018, LIFSHITS' personal accounts at Exchange 3 and Exchange 4 reflected activity from United States IP Addresses 1 and 2. During that same time, including on the same day and within several minutes of one another, the T.W. Exchange 1 Account reflected activity from the same IP addresses.

64. The below table summarizes the IP address activity for LIFSHITS' accounts and the T.W. Exchange 1 Account. For ease of reference, I have highlighted where the LIFSHITS' account and the T.W. Exchange 1 Account were accessed from the same IP address within a few minutes of each other.

UTC Timestamp	IP	IP Activity Type	Account
12/26/2017 11:37:12	United States IP Address 2	Login	LIFSHITS – Exchange 3
12/27/2017 7:51:34	United States IP Address 2	Login	LIFSHITS – Exchange 3
12/28/2017 8:01:51	United States IP Address 2	Login	LIFSHITS – Exchange 3
12/29/2017 7:58:07	United States IP Address 2	Login	LIFSHITS – Exchange 3
12/29/2017 14:43:33	United States IP Address 2	Unknown IP login BEFORE 2FA	T.W. – Exchange 1
12/29/2017 14:44:23	United States IP Address 2	Unknown IP login	T.W. – Exchange 1
12/29/2017 15:31:34	United States IP Address 1	Login before 2FA	T.W. – Exchange 1
12/29/2017 15:31:54	United States IP Address 1	Login	T.W. – Exchange 1
12/29/2017 15:35:40	United States IP Address 1	Login	LIFSHITS – Exchange 3
12/29/2017 15:38:43	United States IP Address 1	Withdrawal 2FA Success[10]	T.W. – Exchange 1
12/29/2017 15:41:24	United States IP Address 1	Logoff	T.W. – Exchange 1
12/29/2017 20:56:07	United States IP Address 1	Login before 2FA	T.W. – Exchange 1

[10] "2FA Success" refers to 2 factor authentication.

UTC Timestamp	IP	IP Activity Type	Account
12/29/2017 20:56:24	United States IP Address 1	Login	T.W. – Exchange 1
12/29/2017 21:01:31	United States IP Address 1	Withdrawal 2FA Success	T.W. – Exchange 1
1/10/2018 16:28:17	United States IP Address 1	Login before 2FA	T.W. – Exchange 1
1/10/2018 16:28:44	United States IP Address 1	Login	T.W. – Exchange 1
1/11/2018 12:23:52	United States IP Address 1	User registration	LIFSHITS – Exchange 4
1/11/2018 12:36:35	United States IP Address 1	Email verification	LIFSHITS – Exchange 4
1/11/2018 12:37:27	United States IP Address 1	User forgot password	LIFSHITS – Exchange 4
1/11/2018 13:49:57	United States IP Address 1	User forgot password	LIFSHITS – Exchange 4
1/12/2018 2:37:29	United States IP Address 1	Login before 2FA	T.W. – Exchange 1
1/12/2018 2:37:43	United States IP Address 1	Login	T.W. – Exchange 1
1/12/2018 2:39:48	United States IP Address 1	Withdrawal 2FA Success	T.W. – Exchange 1

2. Focus on December 29, 2017 Transaction from the T.W. Exchange 1 Account to LIFSHITS' Exchange 3 Account

65. The IP logs of the T.W. Exchange 1 and LIFSHITS' Exchange 3 accounts reflect the following activity on December 29, 2017. This activity indicates that LIFSHITS logged in to his account at Exchange 3 at the same time and from the same IP address as the T.W. Exchange 1 Account, when the latter engaged in a login and subsequent withdrawal of funds:

UTC Timestamp	IP	IP Activity Type	Account
12/29/2017 7:58:07	United States IP Address 2	Login	LIFSHITS – Exchange 3
12/29/2017 14:43:33	United States IP Address 2	Unknown IP login before 2FA	T.W. – Exchange 1
12/29/2017 14:44:23	United States IP Address 2	Unknown IP login	T.W. – Exchange 1
12/29/2017 15:31:34	United States IP Address 1	Login before 2FA	T.W. – Exchange 1
12/29/2017 15:31:54	United States IP Address 1	Login	T.W. – Exchange 1
12/29/2017 15:35:40	United States IP Address 1	Login	LIFSHITS – Exchange 3
12/29/2017 15:38:43	United States IP Address 1	Withdrawal 2FA Success	T.W. – Exchange 1
12/29/2017 15:41:24	United States IP Address 1	Logoff	T.W. – Exchange 1

66. The "Withdrawal 2FA Success" field indicates that on December 29, 2017, at 15:38:43 UTC, the T.W. Exchange 1 Account successfully authorized a withdrawal of funds from the account. The transactional activity of the T.W. Exchange 1 Account confirmed that this withdrawal pertained to the following transaction:

Withdrawal Amount: BTC 0.00938398
Destination Address: [redacted]
Transaction
Hash: [redacted]
Withdrawal Date: 12/29/2017
Withdrawal Time: 15:38:43 (UTC)

67. As noted elsewhere in this Complaint, Exchange 3 records confirm that Destination Address [redacted] is hosted at Exchange 3 and is assigned to LIFSHITS. A review of the transactional activity within LIFSHITS' Exchange 3 account confirmed that the following transaction occurred:

Deposit Amount: BTC 0.00938398
Deposit Address: [redacted]
Transaction
Hash: [redacted]
Deposit Date: 12/29/2017
Deposit Time: 15:57:27 (UTC)

68. Thus, the particular deposit to LIFSHITS' personal Exchange 3 account originated from the T.W. Exchange 1 Account. As established above, Project Lakhta members created the T.W. Exchange 1 Account using a known Project Lakhta email account and the stolen identifiers of T.W., who is a real United States person. Further, in the minutes prior to the transaction, the T.W. Exchange 1 Account reflected an active login session from United States IP Address 1 at the same time that LIFSHITS logged into his personal Exchange 3 account from that same IP address. Several minutes later, the T.W. Exchange 1 Account, using United States IP Address 1, facilitated a transfer of Bitcoin to LIFSHITS' personal Exchange 3 account.

69. I therefore submit that this evidence alone establishes probable cause to believe that LIFSHITS had control of and accessed the T.W. Exchange 1 Account. It also establishes probable cause to believe that LIFSHITS caused the electronic transfer of funds from the T.W. Exchange 1 Account to his (LIFSHITS') own personal account at Exchange 3.

3. Noteworthy Overlaps in User Agent Strings between the LIFSHITS and T.W. Accounts

70. A web browser corresponding to a single user agent string generated the above IP activity at United States IP Addresses 1 and 2, associated with LIFSHITS' Exchange 3 and Exchange 4 accounts between December 26, 2017 and January 11, 2018. With the exception of activity on January 10, 2018, the IP activity associated with the T.W. Exchange 1 Account during that same period was also generated via a browser corresponding to the same user agent string. This means that the internet web browser and version used to access the T.W. Exchange 1 Account and LIFTSHITS' Exchange 3 and Exchange 4 accounts was the same. I submit that when coupled with the fact that the same IP address was used to access the T.W. Exchange 1 Account and LIFSHITS' Exchange 3 account within minutes of each other, the identical user agent strings are further evidence that LIFSHITS used the T.W. Exchange 1 Account to fund his Exchange 3 account.

71. The below table summarizes the IP activity and user agent strings for LIFSHITS' accounts and the T.W. Exchange 1 Account. For ease of reference, I have highlighted the transaction on December 29, 2017.

UTC Timestamp	IP	IP Activity – User Agent String	Account
12/26/2017 11:37:12	United States IP Address 2	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	LIFSHITS – Exchange 3
12/27/2017 7:51:34	United States IP Address 2	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	LIFSHITS – Exchange 3
12/28/2017 8:01:51	United States IP Address 2	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	LIFSHITS – Exchange 3
12/29/2017 7:58:07	United States IP Address 2	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	LIFSHITS – Exchange 3
12/29/2017 14:43:33	United States IP Address 2	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	T.W. – Exchange 1
12/29/2017 14:44:23	United States IP Address 2	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	T.W. – Exchange 1
12/29/2017 15:31:34	United States IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	T.W. – Exchange 1
12/29/2017 15:31:54	United States IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	T.W. – Exchange 1
12/29/2017 15:35:40	United States IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	LIFSHITS – Exchange 3
12/29/2017 15:38:43	United States IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	T.W. – Exchange 1
12/29/2017 15:41:24	United States IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	T.W. – Exchange 1
12/29/2017 20:56:07	United States IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	T.W. – Exchange 1
12/29/2017 20:56:24	United States IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	T.W. – Exchange 1
12/29/2017 21:01:31	United States IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	T.W. – Exchange 1
1/10/2018 16:28:17	United States IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36	T.W. – Exchange 1
1/10/2018 16:28:44	United States IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36	T.W. – Exchange 1
1/11/2018 12:23:52	United States IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	LIFSHITS – Exchange 4
1/11/2018 12:36:35	United States IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	LIFSHITS – Exchange 4
1/11/2018 12:37:27	United States IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	LIFSHITS – Exchange 4
1/11/2018 13:49:57	United States IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	LIFSHITS – Exchange 4
1/12/2018 2:37:29	United States IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	T.W. – Exchange 1
1/12/2018 2:37:43	United States IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	T.W. – Exchange 1

72. As previously stated, a different user agent string was generated on January 10, 2018, when accessing the T.W. Exchange 1 Account. Importantly, this same user agent string appears when LIFSHITS used a Russian IP address to access his Exchange 3 and Exchange 4

accounts during the same time period that the T.W. Exchange 1 Account reflected activity from this user agent string:

UTC Timestamp	IP	IP Activity – User Agent String	Account
1/9/2018 12:19:14	Russian IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36	LIFSHITS – Exchange 3
1/10/2018 16:28:17	United States IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36	T.W. – Exchange 1
1/10/2018 16:28:44	United States IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36	T.W. – Exchange 1
1/19/2018 13:30:38	Russian IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36	LIFSHITS – Exchange 3
1/23/2018 14:44:23	Russian IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36	LIFSHITS – Exchange 3
1/26/2018 13:04:24	Russian IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36	LIFSHITS – Exchange 3
1/29/2018 13:59:34	Russian IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36	LIFSHITS – Exchange 3
2/6/2018 15:14:00	Russian IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36	LIFSHITS – Exchange 3
2/9/2018 18:20:11	Russian IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36	LIFSHITS – Exchange 4
2/15/2018 15:52:57	Russian IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36	LIFSHITS – Exchange 3
2/19/2018 14:56:38	Russian IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36	LIFSHITS – Exchange 3
2/21/2018 14:08:22	Russian IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36	LIFSHITS – Exchange 3
2/22/2018 12:59:00	Russian IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36	LIFSHITS – Exchange 3

73. I submit the use of the same Mozilla user agent string to access both LIFSHITS' Exchange 3 account and the T.W. Exchange 1 Account, during the same time period, provides further supports that LIFSHITS controlled and accessed both accounts.

J. Use of IP Addresses Associated with Computers Located in the Eastern District of Virginia

74. Since 2015, Exchange 2 has used Amazon Web Services ("AWS") for its cloud computing and Application Programming Interface ("API") infrastructure. As part of the conspiracy to commit wire fraud, the conspirators opened three different accounts with Exchange 2 using the means of identification of United States persons, including T.W. The conspirators interacted with and relied upon Exchange 2's AWS infrastructure in order to create, access, and use the Exchange 2 accounts in question. For example, the conspirators used the stolen identifiers of T.W. to create an account with Exchange 2 on March 3, 2017. As part of the account creation process, Exchange 2 used an AWS-controlled IP address in order to deliver a confirmation email to the conspirators so that the latter could complete the account creation by clicking on the email in question. This IP address is associated with a computer located in and operated by AWS from a data center in the Eastern District of Virginia.

75. The conspirators caused Exchange 2 to use IP addresses associated with a computer located in and operated by AWS from its data center(s) in the Eastern District of Virginia on other occasions including, but not limited to, the following:

a. On or about June 28, 2016, Exchange 2 used an AWS-controlled IP address to deliver an account creation verification for an account created using the name of a United States identity theft victim. Further, the conspirators caused Exchange 2 to use IP addresses located in the Eastern District of Virginia on other occasions. For instance, the conspirators linked a United States bank account to this fraudulently obtained Exchange 2 account. This action resulted in Exchange 2 using the AWS infrastructure located in the Eastern District of Virginia to respond to the customer's account activity.